securly://

East Maine School District 63

A case study

June 2020

Table of contents

Chicago area school district uses Securly's Active Directory & Google Authentication solutions in concert to achieve seamless user experience for 4,000 staff and students.

Business challenge

East Maine School District 63 has 7 schools serving 3600 students and 500 staff members. Staff members use Windows devices and students use Chromebooks. Abe Koshy is the network manager for the district. With the district's web filter license expiring in the middle of the year, it was critical for Abe to provide continuity of user experience to his staff members who were used to logging into their Windows machine and be filtered. The existing Fortigate solution offered Windows authentication but, per Abe, suffered from a number of limitations:

Unblocking websites was an extremely tedious process. › Support was extremely hard to get a hold of and a technical resource - even harder. › The product was not K-12 friendly. Educational games for example, would be routinely blocked because they were in the gaming category. No support for Chromebooks, an increasingly important piece of the school network.

Business impact

- Support for both Microsoft and Google single sign-on leads to seamless user experience
- Dramatically improved productivity through selective SSL decryption
- A true 'set and forget' solution means teachers no longer request site unblocks
- User report queries reduced from 2-3 hour task to minutes
- Use of crowdsourced intelligence to keep lists updated with new sites keeps district CIPA compliant

Easy AD SSO setup

The AD SSO setup involves placing a simple ".aspx" ASP.Net script on the school controlled IIS server. All Windows devices logged into the domain automatically pass user information to Securly via this script

Securly has eliminated the load of web filter administration.

It was clear to Abe that the district had to move to a filter that was built for the needs of K-12. The choices came down to a Lightspeed appliance and Securly. Two factors clinched it for Securly - Blended Authentication and Easy SSL Filtering.

Blended authentication: A huge win for user experience

Securly was the only solution that could straddle both the Microsoft and Google worlds with equal ease. The blended authentication approach meant that staff members using Windows devices would be seamlessly authenticated to Active Directory while users of Chrome devices would have the same experience on the Google side.

Active Directory Single-Sign On was an easy implementation aided by a Securly Sales Engineer. While Lightspeed did have a Google authentication solution, Abe found it to be neither easy to implement nor functional. Securly's Chrome extension took 5 minutes to push out to all student OUs and gave Abe the audit data he needed to maintain CIPA compliance while being completely invisible to the user.

Easy SSL Filtering

With 70% of the District's web traffic going over SSL, visibility into this portion of user activity was necessary. The default behavior of the appliance was to decrypt every site. This meant that a never-ending list of exceptions to avoid SSL inspection had to be maintained.

Quick and easy reporting

The Fortinet solution that was replaced by Securly had an on-premise reporting appliance with performance limitations. A single user report would take Abe 2-3 hours to pull. Securly's big data backend is optimized to return quickly on "needle in the haystack" searches. This helps a single user report return in seconds.

> *"Securly's seamless authentication methods have allowed us to provide a great nohassle user experience while giving us granular reporting and policies."*
>
> **Abe Koshy**
> Network Manager

securly://

sales@securly.com

1-855-SECURLY

www.securly.com